# 2019 Capital One Breach Case Study

Student Name: Melissa Gaskins

School of Cybersecurity, Old Dominion University

CYSE 201S: Cybersecurity and the Social Sciences

Instructor Name: Dr. Jordan Quinn

Date: 04/23/2026

## Introduction

In 2019, a previous employee of Amazon Web Services was able to exploit a firewall that was misconfigured due to user error. Using a custom scanning tool she had built, she was able to gain access to many of Capital One's customers' personal information. The stolen data ranged from financial information to social security numbers. According to Petrino, the attack exposed the personal information of people "who had applied for a Capital One credit card between 2005 and 2019" (Petrino, 2026).

## Analysis

According to Petrino, Paige Thompson, a previously employed software engineer of Amazon Web Services "used a technique known as server-side request forgery to extract temporary credentials" that allowed her to gain access to Capital One's "data storage buckets" (Petrino, 2026). Since Thompson had previously worked for AWS, it is possible her previous employment had made it easier for her to perform this attack. However, Capital One did receive some blame due to concerns being ignored by the company. Petrino's article explains that an audit identified the weakness and the company did not proceed with the steps to mitigate it and "failed to establish effective risk assessment processes" before changing their operations to cloud systems. Afterwards, the breach was reported by a user of GitHub who had seen Thompson boasting about it on the platform (Petrino, 2026). It could be assumed that she conducted the attack for personal gain and recognition of her peers.

## Solutions and Barriers

Since the firewall was misconfigured due to human error, one solution could be incorporating stronger user training. However, even with user training there can still be a barrier since human error is very common in cybersecurity, mistakes are bound to happen. Therefore,

the next solution could be stronger risk assessments since Capital One neglected to perform an adequate assessment before transitioning to cloud services. Once again, there can still be barriers due to the company previously ignoring the mistake.

## Reflection

A theory that applies to the incident is Rational Choice Theory which is defined as individuals make choices in their best interest, weighing pleasure versus pain. Since Paige Thompson boasted about the incident on platforms, she most likely believed the benefits of personal gain and recognition outweighed the risk of getting caught. The attack can also be explained by the social science principle of determinism since Thompson was able to easily carry out the attack due to her being previously employed by Amazon Web Services. In other words, her previous employment influenced her decision to attack AWS and Capital One.

## Conclusion

In conclusion, the attack performed by Thompson along with Capital One's negligence allowed her to gain access to sensitive information of the customers of Capital One. This breach sheds light on the fact that it is part of companies' responsibility to assess risks to prevent vulnerabilities from being exposed along with how the social science principle of human factors can influence cybersecurity incidents

## Reference

Petrino, G. (2026, March 26). Capital One Data Breach: What Happened and What to Do | Security.org. Security.org. https://www.security.org/identity-theft/breach/capital-one/